REMARKS

I. INTRODUCTION

Claims 1-4 remain pending in this application. It is respectfully submitted that based on the following remarks that all of the presently pending claims are in condition for allowance.

II. THE 35 U.S.C. § 102(e) REJECTION SHOULD BE WITHDRAWN

The Examiner has rejected claims 1-4 under 35 U.S.C. § 102(e) as unpatentable over U.S. Pat. No. 7,013,391 (Herle). (See 1/12/07 Office Action, pp. 3-5).

Herle describes a mobile station location server that determines the mobile station's location through various location techniques or by receiving the location information from the mobile station over an encrypted channel. The server stores the location in memory that may be accessed by authorized client access devices. A requesting client access device transmits a request to the server. The server authenticates the request to verify that the client access device is authorized to receive the location information. If the client access device is authorized, the server can then transmit the information in either an encrypted or decrypted form to the device. (See Herle, abstract). The server also holds within its memory profile fields of the mobile stations, authorized client profile fields, and encryption-decryption keys. (See Id., col. 5, ll. 55-57). Using the different fields and keys, the server authenticates and transmits the location information. (See Id., col. 5, l. 59 – col. 6, l. 8).

Claim 1 of the present application recites "sharing the predetermined encryption key between the mobile device and the remote terminal but *not* with the server." The Applicant maintains the argument that this recitation highlights the server's minimal interaction when a remote terminal queries the server for the location of the mobile device. For example, if the mobile device and the remote terminal are cellular telephones MS1, MS2, an encryption key may be appended to messages exchanged between the cellular telephones. (See Specification, p. 4, ll. 1-3). Thus, when the remote terminal receives the encrypted location data, "the user of

telephone MS1 [is] able to determine the location of telephone MS2 without a third part being able to do the same." (See Id., p. 4, ll. 22-23). In this manner, the server only provides a route to send the encrypted location data from the mobile device to the remote terminal. That is, the server merely acts as a storage facility for the encrypted location data while the mobile device and the remote terminal possess the means to determine the location of the mobile device.

The system of Herle provides a different approach to providing the location data. Initially, two sets of encryption-decryption keys are utilized. The first encryption-decryption key stored in the memory of the mobile station is used to allow decoding of the location data. The second encryption-decryption key stored in the server is used to authenticate client access devices prior to transmission of the location data. In contrast, the present application utilizes a single encryption key for each query of location data. Furthermore, Herle stores the first encryption key in the memory of the mobile station. Although Herle does not explicitly disclose, it is assumed that the client access device that queries the server for the location data may or may not store the first encryption key. Thus, when a match of the first encryption key occurs, a decryption may take place. However, because the first encryption key is not necessarily "shared" by the mobile station and the client access device, there may be occurrences where the querying client access device is incapable of decrypting the location data. (See Herle, col. 5, ll. 13-19). In contrast, the present application "shar[es] the predetermined encryption key between the mobile device and the remote terminal but not with the server," as recited in claim 1. Therefore, in the present application, the mobile device and the remote terminal always have a common predetermined encryption key that is used to encrypt/decrypt the location data.

In addition, the server of Herle plays a larger role in the location data exchange. Specifically, the *server* of Herle authenticates remote terminals prior to transmission of the mobile station location data. Using the second encryption-decryption key in the mobile station record contained in the memory of the server, the server pre-authenticates the querying client access device prior to transmission of the location data. That is, the server controls the authentication process once the location data is stored in its memory. Herle utilizes a two-tier authentication procedure where the client access device is first authenticated by the server using the second encryption key followed by an enablement for decryption if the first encryption key is

present in the memory of the client access device. The Examiner asserted that Herle does not imply or suggest that the mobile stations share a key with the server, which functions as the provider of the encrypted information upon which both mobile terminals communicate afterward. (See 1/12/07 Office Action, p. 2, l. 22 – p. 3, l. 2). However, in one embodiment of Herle, the first and second encryption keys may further be related if the server decrypts the location data prior to transmission to the client access device. (See Herle, col. 6, ll. 56-60). Because the first encryption key may be shared, the authentication procedure by the server is necessary. In contrast, claim 1 of the present application recites "sharing the predetermined encryption key between the mobile device and the remote terminal but not with the server." Thus, no authentication procedure is required at the server since only the remote terminal with the encryption key may decode the encrypted location data. As discussed above, the server provides a conduit to store and transmit the encrypted location data, not as an authentication level. That is, the encryption key is present at the mobile device and the remote terminal that an authentication procedure by the server is unnecessary.

Thus, it is respectfully submitted that Herle does not disclose or suggest "sharing the predetermined encryption key between the mobile device and the remote terminal but *not* with the server," as recited in claim 1. Accordingly, it is respectfully requested that the Examiner should withdraw the 35 U.S.C. § 102(e) rejection of claim 1.

Claim 2 recites a "mobile device configured to…share the predetermined encryption key with a remote terminal but not the server." Thus, it is respectfully submitted that this claim is also allowable for the same reasons discussed above with reference to claim 1. Accordingly, it is respectfully requested that the Examiner should withdraw the 35 U.S.C. § 102(e) rejection of claim 2.

Claim 3 recites a server "wherein between receipt and transmission of the encrypted location by the server, the server is not in possession of the encryption key." Thus, it is respectfully submitted that this claim is also allowable for the same reasons discussed above with reference to claim 1. Accordingly, it is respectfully requested that the Examiner should withdraw the 35 U.S.C. § 102(e) rejection of claim 3.

Claim 4 recites a "terminal configured to query a remote server for the location of a particular mobile device with which it has shared an encryption key independently of the server." Thus, it is respectfully submitted that this claim is also allowable for the same reasons discussed above with reference to claim 1. Accordingly, it is respectfully requested that the Examiner should withdraw the 35 U.S.C. § 102(e) rejection of claim 4.

CONCLUSION

In view of the above remarks, it is respectfully submitted that all the presently pending claims are in condition for allowance. All issues raised by the Examiner having been addressed, an early and favorable action on the merits is earnestly solicited.

Please direct all future correspondence to:

Paul Im, Esq.
IP Counsel

Philips Intellectual Property & Standards
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9602
Fax: (914) 332-0615
Email: Paul.im@philips.com

Respectfully submitted,

Dated: February 13, 2007

By: _____
Oleg F Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, New York 10038
Tel: (212) 619-6000
Fax: (212) 619-0276